Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 21 June 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Associated Press reports that the drought gripping the Western United States could be the biggest in 500 years, with effects in the Colorado River basin considerably worse than during the Dust Bowl years. (See item 17)
- The Associated Press reports that at least 240 people are telling health officials they got sick after eating at a restaurant in Fort Collins, CO. (See item 20)
- The Christian Science Monitor reports that the kidnapping and beheading of American Paul Johnson Jr. marks a turning point in Saudi public opinion against his al Qaeda slayers. (See item 30)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 19, Associated Press* — **Fire at nuclear power plant. The Vermont Yankee nuclear power plant in Vernon, VT, was shut down Friday, June 18, after a transformer caught fire in a non−nuclear part of the plant,** officials said. The fire was put out, and no radiation was released, they said. The operators declared an "unusual event," the lowest of four emergency classifications set by the federal Nuclear Regulatory Commission. The nuclear reactor was automatically shut down as soon as the fire was detected, plant spokesperson Rob Williams said. **The cause of the blaze had not been determined.** Ten to 20 gallons of oil from

the transformer flowed into the Connecticut River through a storm drain, Williams said. A clean−up crew was called in to contain the spill. The transformer is used to step up the voltage of the electricity generated at the plant so it can be transmitted more efficiently. Officials did not know how badly it was damaged, and Williams said he could not estimate when the plant might be back on line again. Williams said the transformer was installed less than two years ago.
Source: http://edition.cnn.com/2004/US/Northeast/06/18/nuclear.plant .fire.ap/

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *June 19, Middletown Press (CT)* — **Chlorine gas threat. Fears that a graphite purifying cylinder could explode igniting chlorine gas, resulted in the evacuation of residents within a mile of Graphite Die Mold Inc., in Durhan, CT, late Friday, June 18.** All roads leading up to the facility were closed off as the hazmat teams from the Department of Environmental Protection did a walk through, fearing that the oven wasn't releasing enough pressure. Graphic Die Mold, a subsidiary of The Morgan Crucible Co. plc, manufactures high precision graphite products "for a wide variety of applications," according to the company's Website.
Source: http://www.middletownpress.com/site/news.cfm?newsid=12014794 &BRD=1645&PAG=461&dept_id=10856&rfi=6

[Return to top]

Defense Industrial Base Sector

3. *June 18, Washington Technology* — **Navy to spend $95 million on jamproof communications. The Navy's Space and Naval Warfare Systems Command has awarded a pair of delivery orders for multifunctional information distribution system terminals, according to a Department of Defense statement. The low−volume terminals (LVTs) provide secure, high−capacity, digital data and voice communications that are resistant to enemy jamming.** They are used in Navy, Air Force and Army communications platforms. The Navy is purchasing LVT1 terminals, which go into airborne platforms, and LVT2 terminals, which are land−based. ViaSat is the only provider of government−certified LVT2 terminals. The terminals will go into a variety of platforms, including the F−16, F−18 and Thunderbolt II aircraft, and the Black Hawk helicopter. On land, the terminals will help power a variety of communications, including the Army Tactical Radio Communication System and the Joint Unmanned Combat Air System. Included in the two Navy orders are purchases for the governments of Belgium, Canada, Japan, Poland, Switzerland and Taiwan. The Navy expects delivery to be completed by May 2006.
Source: http://www.wtonline.com/news/1_1/daily_news/23829−1.html

4. *June 18, New York Times* — **Senate votes to increase Army troop strength. The Senate voted overwhelmingly on Thursday, June 17, to increase the strength of the Army by 20,000 soldiers, with lawmakers saying the military is badly strained by operations in Iraq and Afghanistan.** Members of both parties said the troops, added to the Pentagon spending

plan for 2005 on a 93−to−4 vote, were essential in light of international tensions and the policy of keeping military personnel in Iraq and elsewhere beyond their scheduled tours. Senators have been pressing for a personnel increase as well as for dispatching more forces to Iraq. The administration has resisted, saying the army has enough. Under a compromise, the Senate agreed to pay the $1.7 billion cost of the new personnel out of the administration's $25 billion request for operations in Iraq and Afghanistan through early next year. **The additional soldiers would bring the authorized strength of the Army to 502,400.** The House also approved additional troops, but phased them in over three years.
Source: http://www.nytimes.com/2004/06/18/politics/18spend.html

[Return to top]

Banking and Finance Sector

5. *June 18, Knight Ridder Tribune* — **Identity theft more prevalent in NFL than other pro sports. National Football League (NFL) director of security Milt Ahlerich said cases involving identity theft and impersonation fraud have increased dramatically in recent years and are now the most common way that NFL players are victimized.** Impersonation fraud and identity theft aren't unique to the NFL, but National Basketball Association (NBA) and Major League Baseball security officials confirmed that they don't handle the volume of cases that Ahlerich does. People have impersonated athletes for years, but Ahlerich has spotted a recent trend. Perpetrators are no longer just trying to impress bar patrons, they are targeting players for the sole purpose of committing fraud. **Impersonators usually target lesser−known players instead of more recognizable superstars. They are well versed on details of the player's career and often carry forged documents.** Identity theft victims spend an average of 600 hours recovering from the crime, according to statistics provided by the Identity Theft Resource Center.
Source: http://www.mercurynews.com/mld/mercurynews/sports/8955020.ht m?1c

6. *June 18, Associated Press* — **Survey: credit reports have errors. One in four credit reports has errors that are serious enough to disqualify consumers from buying a home, opening a bank account or getting a job −− and an overwhelming majority contain mistakes of some kind**, according to a survey released Thursday, June 17, by a consumer group. Of the 197 credit reports collected from people in 30 states, 79 percent had some sort of error, said the report by Public Interest Research Group (PIRG). The three largest credit−reporting agencies −− Equifax, Experian and Trans Union −− collect information from banks, and other creditors, and from public records. The people who provided information for the survey were members of PIRG −− an arrangement that a spokesperson for the credit−reporting industry said unfairly skewed the results. Also, in conducting the survey, PIRG "unilaterally decided what is a serious error," said Norm Magnuson of the Consumer Data Industry Association. PIRG and other groups advise consumers to examine their reports from all three credit bureaus at least once a year before applying for new credit. The reports are available without charge in several states, and will be provided free nationwide by late next year. Survey:
http://uspirg.org/reports/MistakesDoHappen2004.pdf
Source: http://www.nytimes.com/aponline/business/AP−Credit−Report−Er rors.html

7.

June 17, Federal Trade Commission — **Phishers settle Federal Trade Commission charges.** Operators who used deceptive spam and copycat Websites to con consumers into turning over confidential financial information, also called phishing, have agreed to settle Federal Trade Commission charges that their scam violated federal laws. **The two settlements announced on Thursday, June 18, will bar the defendants from sending spam, bar them from making false claims to obtain consumers' financial information, bar them from misrepresenting themselves to consumers, and bar them from using, selling, or sharing any of the sensitive consumer information collected.** Based on financial records provided by the defendants, the FTC agreed to consider the $125,000 judgments in each case satisfied. If the court finds that the financial documents were falsified, however, the defendants will pay $125,000 in consumer redress. One of the defendants also faces 46 months in prison on criminal charges filed by the Justice Department. The defendant named in one of the complaints is Zachary Keith Hill. The Hill case was filed in December 2003, in the U.S. District Court for the Southern District of Texas. The other case, filed in May 2004, charged an unnamed minor in U. S. District Court for the Eastern District of New York.
Source: http://www.ftc.gov/opa/2004/06/hill.htm

8. *June 17, Washington Post* — **Feds, private groups to educate consumers about phishing scams. The federal government and some of the nation's leading consumer organizations and financial institutions on Thursday, June 17, kicked off a campaign to educate consumers about the growing threat posed by "phishing," a sophisticated form of identity theft conducted via e−mail and counterfeit Websites.** Visa USA, the Federal Trade Commission, the Better Business Bureau and the other coalition members said they plan to work together to teach consumers how to avoid phishing scams and to report suspicious e−mail to authorities. **The combination of law enforcement and public outreach is needed to tackle phishing, said Wayne Abernathy, the assistant secretary for financial institutions at the Department of Treasury**. Call for Action, an international clearinghouse for consumer information, is providing a free identity theft hotline (1−866−ID−HOTLINE). Howard Beales, director of the Federal Trade Commission's Bureau of Consumer Protection, encouraged Americans to forward any suspicious e−mail messages to the FTC at uce@ftc.gov. Such information is valuable, he said, because it helps investigators track scam artists, many of whom change their Website locations and e−mail addresses frequently in an effort to frustrate law enforcement officials.
Source: http://www.washingtonpost.com/wp−dyn/articles/A49911−2004Jun 17.html

[Return to top]

Transportation Sector

9. *June 21, Associated Press* — **Airliner lands at wrong airport. A Northwest Airlines flight that was headed to Rapid City, SD, landed a few miles off course at Ellsworth Air Force Base, and passengers had to wait in the plane for more than three hours while their crew was questioned.** Passengers on Northwest Flight 1152, an Airbus A−319 from St. Paul, MN, expected to be welcomed to Rapid City Regional Airport on Saturday, June 19, but after about five minutes they were told to close their window shades and not look out, said passenger Robert Morrell. Eventually, the captain and first officer were replaced by a different Northwest crew for the short hop to the right airport. Northwest confirmed that the crew made an

"unscheduled landing." The Federal Aviation Administration is investigating.
Source: http://www.cnn.com/2004/US/Central/06/20/wrong.airport.ap/in dex.html

10. *June 19, Associated Press* — **Inspection of all air cargo too costly, House decides in defeating proposal . The House refused on Friday, June 18, to require inspections of all cargo shipped on passenger−airline flights, heeding arguments that the technology is not available, and losing the freight would drive carriers into bankruptcy.** Only a small percentage of cargo aboard passenger flights is inspected, and uninspected cargo is supposed to come only from shippers known to the government. Rep. Harold Rogers referred to estimates by the Transportation Security Administration that it would take $700 million and the hiring of 9,000 additional inspectors to examine cargo thoroughly on passenger flights at the nation's largest airports. He said that forbidding airlines to carry uninspected freight would have financially catastrophic effects on an industry that already has several struggling companies.
Source: http://www.journalnow.com/servlet/Satellite?pagename=WSJ%2FMGArticle%2FWSJ_BasicArticle&c=MGArticle&cid=1031776142832&path=!nationworld&s=1037645509161

11. *June 18, Government Computer News* — **Rail security bill introduced.** House Transportation and Infrastructure Committee leaders introduced legislation in the House of Representatives yesterday designed to protect the passenger and freight rail systems from terrorist attack. The Protecting Railroads against Enemy Efforts through Modernization, Planning and Technology Act (H.R. 4604) would provide resources to harden the railroads against attack such as the one in Madrid, Spain, and to improve operational recovery from such an incident. **The legislation will fund new technologies such as automated freight car inspection, right−of−way track security monitoring and emergency bridge repair systems. The legislation will provide more than $1 billion in new money,** including more than $600 million to improve rail tunnels that Amtrak and commuter railroads use. The Department of Transportation will work with the Department of Homeland Security on establishing responsibilities for the security plan provisions in the legislation.
Source: http://www.gcn.com/vol1_no1/daily−updates/26252−1.html

[Return to top]

Postal and Shipping Sector

12. *June 16, DM News* — **USPS board approves capital projects.** The U.S. Postal Service (USPS) Board of Governors approved several major capital projects at its monthly meeting Tuesday, June 15, including the third phase of its Surface Air Support System (SASS). **In the first phase, an infrastructure was developed to track FedEx and Amtrak shipments. In the second phase, SASS was expanded to include commercial air visibility. In the latest phase, wireless scanners will be used to track several visibility points, from container loading to the unloading of both USPS and postal customer trailers.** The system will be deployed at 129 facilities. The board also approved money to increase efficiency in its automation system by purchasing 1,587 stacker modules and 2,041 tray carts, which will help letter mail be sorted to Delivery Point Sequence, the order in which letter carriers deliver the mail. ·
Source: http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2862 7

[Return to top]

Agriculture Sector

13. *June 17, Associated Press* — **Outbreak of FMD in Brazil. Brazilian officials confirmed an outbreak of foot−and−mouth disease (FMD) in an Amazon state, the Agriculture Ministry has said.** The ministry was warned about a possible outbreak of the disease on June 12 and tests came back positive Wednesday, June 16, for three of the 130 cows on the farm in question. In a statement, the ministry denied the outbreak would hinder the country's efforts to eradicate the disease by 2005. **Brazil has the world's largest beef herd with 182 million head of cattle and the ministry says the herd is 88 percent free of the disease.** FMD is a highly contagious viral disease and affects cloven−hoofed animals like cattle, sheep, and pigs. It causes sores, blisters and fever. The last outbreak of FMD in Brazil was 34 months ago in northeastern Maranhao state.
Source: http://www.ndtv.com/template/template.asp?template=Health&slug=Outbreak+of+FMD+in+Brazil&id=55731&callid=1

14. *June 17, Radio Australia* — **FMD affects two Cambodian provinces. More than 2,000 cows and buffalos have been infected with foot and mouth disease (FMD) in two Cambodian provinces west of the capital, Phnom Penh.** An animal health official in Kampong Chhang province says the disease hit two districts in May, infecting about 2,000 animals, but has now been contained. The official says experts have been deployed to advise farmers on preventing the spread of the disease. He says FMD may have spread from Kampong Speu province, which had an outbreak in February and another one earlier this month, due to heavy rains.
Source: http://www.abc.net.au/ra/newstories/RANewsStories_1134406.ht m

[Return to top]

Food Sector

15. *June 18, Food Production Daily* — **Essential oils to fight food bacteria. A study from the University of Southampton in the UK reveals that candles and ion wind delivery systems containing certain essential oils can reduce a range of commonly found bacteria in foodstuffs −− a system that could provide a cheap and effective means for food manufacturers to reduce bacterial risk.** The researchers, Lindsey Gaunt and Sabrina Higgins, have discovered that by adding certain essential oils to the candle it can destroy bacteria such as Escherichia Coli and Staphylococcus aureus on surfaces. Gaunt and Higgins have been testing different essential oils, such as orange, thyme, and eucalyptus, which when dispersed into the air and combined with the ions produced in the candle flame, have a powerful bactericidal effect. Where candle use would not be appropriate, for example in a kitchen, the same bactericidal effect can be produced by using plug−in devices combining the appropriate essential oils and ions generated by an electrical discharge. According to Gaunt, the candles and electrical devices could be as effective as liquid disinfectants, together with the added benefit of being able to penetrate porous surfaces and fabrics in a room with very little personal effort.
Source: http://www.foodproductiondaily.com/news/news−NG.asp?id=52939

16. *June 17, Yale University* — **Salmonella research. Researchers at the Yale School of Medicine report a new and fundamental mechanism that Salmonella bacteria use to replicate within body cells and cause disease without endangering themselves.** Most dangerous bacteria that enter the body are engulfed and digested by cells called macrophages. Once inside a macrophage, the bacteria are targeted for death by a mechanism that transports them within a vesicle to a specialized compartment, the lysozome, designed to degrade foreign or unwanted materials. Once the bacterium is engulfed, it takes only about 30 minutes to reach a lysozome. Therefore, to survive and replicate, bacteria must act rapidly to avoid this pathway to degradation. Salmonella, the bacterium that causes food poisoning, can do that. The Salmonella bacteria use a "syringe−like" device called the type III secretion system to deliver a protein, SopB, which has phosphoinositide phosphatase activity and modifies the composition of the vacuole that encloses them.
Source: http://www.eurekalert.org/pub_releases/2004−06/yu−sic061704. php

[Return to top]

Water Sector

17. *June 18, Associated Press* — **Western drought. The drought gripping the Western U.S. could be the biggest in 500 years, with effects in the Colorado River basin considerably worse than during the Dust Bowl years, scientists at the U.S. Geological Survey (USGS) said Thursday, June 17.** The Colorado River has been in a drought for the entire decade, cutting an important source of water for millions of people across the West, including Southern California. The report said the river had its highest flow of the 20th century from 1905 to 1922, the years used to estimate how much water Western states would receive under the Colorado River Compact. The report is available at http://water.usgs.gov/pubs/fs/2004/3062/
Source: http://story.news.yahoo.com/news?tmpl=story&cid=624&e=3&u=/ap/20040618/ap_on_sc/record_drought_4

[Return to top]

Public Health Sector

18. *June 18, Medical News Today* — **Scientists learn how adjuvant makes vaccines effective.** Eighty years after adjuvants were first used to boost the effectiveness of vaccines, researchers at the National Jewish Medical and Research Center have finally begun to understand how they work. **They report that the most common adjuvant, alum, provokes a previously unrecognized group of immune−system cells to secrete the protein interleukin−4, which primes B cells for a better response to the vaccine.** Live vaccines, containing weakened forms of an infectious organism, generally work fine by themselves. But vaccines containing dead organisms (inactivated vaccines) or pieces of the infectious organisms or their toxins (acellular or recombinant vaccines) generally need adjuvants to boost their effectiveness. The National Jewish team was investigating a phenomenon known as MHC class II signaling, which occurs during interactions between B cells and T cells. Researchers noticed that B cells must be prepared, or primed, if they are to be stimulated through this signaling pathway. If not

primed, they will do nothing or even self−destruct. **"Our findings will lead us in the future to better understand how adjuvants have helped prevent disease. By understanding how they work we may be able to design new and more effective adjuvants," said John Cambier, Chairman of the Integrated Department of Immunology at National Jewish.**
Source: http://www.medicalnewstoday.com/medicalnews.php?newsid=9615

19. *June 18, BBC News* — **Superbug deaths set to double. United Kingdom scientists say methicillin−resistant Staphylococcus aureus (MRSA) is becoming increasingly resistant to the antibiotic vancomycin.** It had been thought that vancomycin−resistance was only a problem in one strain of MRSA −− seen in the U.S. and Japan. But scientists from the University of Bath, University of Bristol, and Southmead Hospital say all five major types of MRSA show signs of resistance to vancomycin. The study was carried out in the UK, USA, France, Japan, Sweden, Poland, Norway, and China. Three cases of MRSA bacteria which are totally resistant to vancomycin have been reported in the U.S. The type of bacteria with increased resistance is known as VISA −− vancomycin−intermediate Staphylococcus aureus. The scientists believe that it may be an intermediate stage to the development of bacteria which are fully resistant to vancomycin. Mark Enright of the University of Bath who led the research, told BBC News Online: **"With increasing vancomycin−resistance, we are going to see a significant increase in mortality. "If we lose vancomycin completely as a treatment, we could see a doubling in deaths over the next five years."**
Source: http://news.bbc.co.uk/1/hi/health/3818277.stm

20. *June 18, Associated Press* — **People sickened at Colorado restaurant. At least 240 people are telling health officials they got sick after eating at a restaurant in Fort Collins, CO.** The outbreak is so large that ten county employees have been assigned to the investigation. People who ate at the Texas Roadhouse say they've been experiencing cramps, diarrhea, vomiting, and other symptoms within 48 hours of their meals. The steak house is part of a national chain based in Louisville, KY. Health officials say the restaurant is closed temporarily and that the company has hired a private contractor to disinfect it. **They say the virus appears to be the same one that sickened hundreds of people on a cruise ship docked in Alaska earlier this month.**
Source: http://www.kpvi.com/index.cfm?page=nbcheadlines.cfm&ID=19427

21. *June 18, New Mexico Channel* — **Treatment tested for West Nile virus. A Boston−area West Nile virus patient is trying an experimental treatment to manage the potentially deadly illness.** At the age of 71, Thomas Cook was an avid hiker, bicyclist, and roller blader. Now, he needs crutches to help him walk. About 90 percent of people who contract West Nile virus never even show symptoms. Only a small number of people will become seriously ill. But of those, many people with significant central nervous system or neurological involvement with West Nile viral infections die. There's no real treatment for West Nile virus, but Cook said that the drug Cozar is helping. It belongs to a group of medications called "ACE inhibitors," which are usually prescribed to people with high blood pressure or diabetes. **Now, a new study is looking to see whether ACE inhibitors can help fight the West Nile virus.**
Source: http://www.thenewmexicochannel.com/health/3433457/detail.htm l

[Return to top]

Government Sector

22. *June 18, Department of Homeland Security* — **Department of Homeland Security announces first Designations and Certifications under the Safety Act. The Department of Homeland Security announced the issuance of Designations and Certifications for four anti−terrorism technologies under the Support Anti−terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act).** This is the first announcement in an ongoing process of review, analysis, and designation and certification of anti−terrorism technologies. The four technologies include an integrated computer system that provides near real−time, event−driven terrorism threat analysis, allowing the focus of resources on the most imminent threats and greatest risks. They also include a two−way high−speed video/audio system designed to allow off−site bomb technicians to support clients in x−ray screening of items for explosives and hazardous materials through real−time viewing of images of suspicious items; as well as, a biohazard detection system that detects trace levels of DNA from anthrax spores and other biological agents as mail is processed on high−speed sorting equipment. Additionally, a remotely operated, ultra−high pressure water jet cutting system designed to investigate and aid in the neutralization of explosive devices by providing a rapid means of gaining access to the interiors of devices has recieved certification.
Source: http://www.dhs.gov/dhspublic/display?content=3726

23. *June 18, Federal Computer Week* — **Group recommends DHS grant exemption. Officials from the Task Force on State and Local Homeland Security Funding Friday, June 18, delivered to Department Homeland Security (DHS) Secretary Tom Ridge a report on why local government officials haven't seen the DHS money they expected.** The document includes 15 recommendations for getting past those problems. At the end of its three−month investigation, the task force blamed hang−ups in the funding on years of grants management, procurement laws and practices, and other policies designed to ensure that government money is spent appropriately. **The group's top recommendation is to exempt fiscal 2005 grants from the federal Cash Management Improvement Act of 1990 in a trial run at allowing local agencies to receive the money up to 120 days before they have to spend it.** That would help cities whose charters forbid them from signing contracts unless the money is actually in their account. Communities also should follow the other recommendations, said Donald Plusquellic, mayor of Akron, Ohio and vice chairman of the task force. That includes having legislatures and public officials exercise emergency procurement authority while working out permanent solutions for homeland security buys, and getting officials from multiple jurisdictions to use each others' contracts.
Source: http://www.fcw.com/fcw/articles/2004/0614/web−dhs−06−17−04.a sp

[Return to top]

Emergency Services Sector

24. *June 19, The Cincinnati Enquirer* — **City rescue squads strained. Cincinnati, OH, struggling to figure out how to respond to more ambulance calls with less money, already lags behind many other cities in the number of ambulances per resident.** The Cincinnati Fire Department operates 10 ambulances from firehouses in the city − one for every 31,128

residents. And a growing number of calls seeking medical care made them unavailable last year an average of 1 1/2 times every day. For years, firefighters have complained about too many calls for medical help and too few people to handle them effectively. Cincinnati ambulances got 50,000 calls last year and transported patients to hospitals in a little more than half of those cases. **Ambulances were unavailable in the city 574 times last year.** Experts say there's no clear standard on how many ambulances a community should have. The American Ambulance Association recommends at least one ambulance for every 25,000 people.
Source: http://www.enquirer.com/editions/2004/06/19/loc_ambulance19. html

[Return to top]

Information Technology and Telecommunications Sector

25. *June 21, Computerworld* — **NYC wireless network will be unprecedented. New York City plans to build a public safety wireless network of unprecedented scale and scope, including the capacity to provide tens of thousands of mobile users with the ability to send and receive data while traveling at speeds of up to 70 mph citywide.** Bids from vendors are due next month, and Gino Menchini, commissioner of the city's Department of Information Technology & Telecommunications, said he expects to award contracts for three−month pilot projects to multiple bidders by year's end. The final contract is expected to cover five years, with options for two five−year renewals. Menchini said **the network would provide mobile users from the New York police, fire and emergency medical service departments with broadband access to information such as mug shot and fingerprint databases and building floor plans**. The city also wants to use the network to control traffic signals and support an automatic vehicle−location system that would be tied into its dispatch systems. Plans call for the wireless network to support up to 5,000 end users initially and then be expanded.
Source: http://www.computerworld.com/mobiletopics/mobile/story/0,108 01,93952,00.html

26. *June 18, Computerworld* — **Speed record set for public network data transfer.** The Swedish National Research and Education Network (Sunet) and Sprint Corp. announced Friday, June 18, that they have set a world record for transporting a large volume of data over a public network. The companies said **they sent nearly 840GB of data from a computer in San Jose, CA, to another one 10,000 miles away at the University of Lulea in northern Sweden in less than 27 minutes**. That much data is equivalent to 140 full−length movies in digital form. The data transfer shows how companies and organizations with mountains of data can use the Internet to provide disaster recovery and off−site storage functions quickly, Sprint officials said. **The transfer, done in April and validated only recently, is about three times faster than the current record listed in the 2004 edition of the Guinness Book of World Records.** The data was transmitted over the public network while it was being used by other customers of the two companies.
Source: http://www.computerworld.com/networkingtopics/networking/sto ry/0,10801,93947,00.html

27. *June 18, eWEEK* — **Report: VOIP phones won't gain lead until 2009.** In a report issued Thursday, June 17, telecommunications market research firm Insight Research found that VOIP phones in the enterprise will not outnumber the installed PBX base until 2009. **According to the study, the PBX business will ship about $4.3 billion worth of PBX equipment this year.**

The cost of IP phones, at 25 percent more than that of their digital counterparts, is a factor slowing uptake, said Bob Rosenberg, president of Insight. But VOIP's support for integrated vertical telephony applications is a potent lure. Newer VOIP PBX phones are expected to grow at a compounded rate of more than 20 percent over the forecast period, while the older TDM (time−division multiplexing)−based phone technology declines at roughly the same rate. A similar replacement process dictates outsourced switching alternatives: Traditional Centrex has declined from a high of 17.3 million lines in 2001 to a predicted 13.3 million at the end of 2004. "We're predicting a 1.5 million−line IP Centrex installed base by the end of the year," Rosenberg said. Study: http://www.insight−corp.com/pr/06_16_2004.asp
Source: http://www.eweek.com/article2/0,1759,1614773,00.asp

28. *June 18, Associated Press* — **Another technical glitch slows Yahoo!** Some Yahoo! Inc. Websites and services stumbled for the second time in less than a week Thursday, June 17, as the company worked to resolve a hardware problem. **In the latest glitch, users may have experienced a slow response from the company's servers from about 11 a.m. EDT to 1 p.m. Some people also reported that they were unable to log onto Yahoo's instant messaging program.** The company released a statement describing the problem as an "isolated hardware−related issue." It was unrelated to Tuesday's incident in which Yahoo and several other Websites were sluggish or entirely inaccessible for two hours.
Source: http://www.nytimes.com/aponline/technology/AP−Yahoo−Slowdown .html

29. *June 17, Mobile Pipeline* — **Vendor claims hackers can hijack hotspot authentication .** A security flaw in some implementations of Bluetooth enables hackers to easily steal Wi−Fi hotspot authentication information, UK security firm Integralis said Thursday, June 17. The Bluetooth flaw is exploited when users sign up for hotspot access using SMS text messaging, a method allowed by a variety of hotspot providers. The flaw enables nearby hackers to intercept the SMS message containing log−on information as it travels between the user and the hotspot vendor, according to the company. The company said it found the potential problem exists with a variety of operators including Cingular in the U.S., and T−Mobile and Vodafone in Europe. **The company said the attack can be automated and accomplished in under a minute. It said it had no evidence that such attacks have actually occurred.**
Source: http://informationweek.securitypipeline.com/news/22100494

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

Watch Synopsis: Internet scans for backdoor and Trojan Horse ports continue to top the lists of all reporting organizations. The likely reason for such scans are that Bot Networks continue to amass zombie hosts from prior infected hosts such as Sasser and Bagel victims. The use of "botnets" to create denial of service attacks remain a serious threat to the National Infrastructure.

Current Port Attacks

Top 10 Target Ports	9898 (dabber), 5554 (sasser−ftp), 445 (microsoft−ds), 1026 (nterm), 1023 (Reserved), 135 (epmap), 1434 (ms−sql−m), 3127 (mydoom), 1433 (ms−sql−s), 1027 (icq) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

General Sector

30. *June 21, The Christian Science Monitor* — **Al Qaeda terror riles Saudi public.** The kidnapping and beheading of American Paul Johnson Jr. marks a turning point in Saudi public opinion against his al Qaeda slayers. **Celebrations broke out at the news Friday, June 18, that Abdelaziz al−Miqrin, the man responsible for Johnson's death, and three other al Qaeda linked members had been killed. It was the first time in the kingdom's 13−month fight against terrorism that ordinary citizens expressed spontaneous joy at security forces' success.** If popular sentiment turns away from jihadists, analysts say, it could undermine their ability to find support in the form of hiding places and suicide cars. The group's strength lies not only in its leadership but in its ability to draw new recruits. Two of the men killed Friday, including a teenager, were not on the list of wanted suspects. Over the past year, many of the dozens of suspected terrorists arrested or killed in shootouts were also not on the list posted by the Interior Ministry. **Analysts cite several reasons for al Qaeda's appeal. There is high unemployment, an uneven distribution of wealth, and a lack of alternative sources for peaceful dissent**, says Fahd al−Shafi, a former extremist who knew Miqrin in the 1990s.
Source: http://csmonitor.com/2004/0621/p01s02−wome.html

31. *June 18, Voice of America* — **Pakistani security forces kill al Qaeda facilitator. Security forces in Pakistan have killed a rebel tribal leader in an operation against al Qaeda−linked terror suspects in a remote mountainous region. Pakistani officials say that nearly 70 suspected terrorists have been killed in the area in less than two weeks.** Officials and witnesses say Nek Mohammad was killed, along with four associates, in a late night rocket attack near the Afghan border. The military described the 27−year−old Mohammad as an al Qaeda facilitator. "We had the information about presence of Nek Mohammad and his associates in this particular area, which was targeted last night, and it is believed that he is amongst those five killed," explained Major−General Shaukat Sultan, chief spokesman for the Pakistan army. **Mohammad was allegedly sheltering and protecting dozens of suspected foreign al Qaeda militants in the area.**
Source: http://www.voanews.com/article.cfm?objectID=BC70B3D5−48BB−4EED−89EB78480632915E

32. *June 17, Associated Press* — **'Dr. Chaos' sentenced to nearly 21 years. A man who admitted hiding deadly cyanide in a Chicago subway tunnel in 2001 was sentenced to nearly 21 years in prison Thursday, June 17, for conspiring to knock out power lines, burn buildings and damage computers in Wisconsin.** Joseph Konopka, 27, who calls himself "Dr. Chaos," will serve the first 11 years of the sentence at the same time he finishes the

13−year prison term from Illinois. He will serve about 23 years in prison. U.S. District Judge Lynn Adelman also ordered him to pay more than $435,000 in restitution to various victims. Authorities said **more than 50 acts in various Wisconsin counties affected more than 30,000 power customers and caused more than $800,000 in damages.** Prosecutors said Konopka was the self−appointed leader of a loose affiliation called "The Realm of Chaos," which recruited youths to engage in property damage. Konopka was sent to prison last year for taking two bottles of cyanide from an abandoned chemical warehouse and hiding them in the subway. He said he had considered using the cyanide to commit suicide.
Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−brf−dr−chaos,0,3910767.story?coll=sns−ap−nation−headlines

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is an internal DHS/IAIP tool intended to serve the